УПРАВЛЕНИЕ ДОСТУПОМ

УДК 004.056
DOI: 10.52190/2073-2600_2021_3_3

Интеграция СЗИ со службой каталогов Astra Linux Directory: проблемы и подходы

А. О. Лобач
Московский физико-технический институт (национальный исследовательский университет), г. Долгопрудный, Московская обл., Россия

Сформулирована обобщенная схема идентификации/аутентификации (И/А) средств защиты информации (СЗИ). Проведен обзор каталога Astra Linux Directory (ALD). С учетом проведенного анализа предложены и рассмотрены подходы к решению задачи интеграции СЗИ и ALD. В каждом из подходов выделены этапы И/А СЗИ, которые переходят на сторону ALD при их интеграции. Сформулированы общие алгоритмы реализации данных подходов. Выявлены основные проблемы и угрозы выбранных подходов.

Ключевые слова: система защиты информации, Astra Linux Directory, аутентификация, идентификация, угрозы.

При интеграции СЗИ с экосистемой (совокупность сервисов, устройств, прочих продуктов, поддерживаемых одной или разными компаниями и неразрывно связанных в единую сеть определенными организационными и/или технологическими процессами [1]) особое внимание необходимо уделить реализации основных функций защиты от несанкционированного доступа. Прежде всего это идентификация и аутентификация, функции, позволяющие зафиксировать круг лиц, имеющих доступ к объекту, который защищает СЗИ, а также функция разграничения доступа, которая непосредственно определяет права пользователей, прошедших И/А [2].

В свою очередь политика безопасности и правила разграничения доступа формируются на более высоком уровне абстракции по сравнению с уровнем, на котором выполняют базовые функции СЗИ [3]. Современные экосистемы стремятся проводить настройку прав и атрибутов доступа в одном месте с настройкой параметров И/А [4], поэтому возникает необходимость встраивания СЗИ в существующие экосистемы. При таком встраивании часть базовых функций СЗИ будет выполняться в отдельных компонентах данной экосистемы, что может создать дополнительные угрозы, которые не рассматривали при разработке СЗИ. В результате необходимо разобрать, какие способы встраивания СЗИ в экосистему существуют и к проявлению каких угроз они могут привести. Важными условиям этого встраивания являются сохранение высокого уровня безопасности существующих СЗИ и реализация компенсационных мер для вновь появившихся угроз.

В данной статье в качестве примера СЗИ рассматриваются системы линейки Аккорд, которые являются одними из лидирующих продуктов на российском рынке.

В качестве примера экосистемы рассматривается комплекс программ ALD. Стоит отметить, что на текущий момент анонсирован выход новой версии — ALD Pro. Про данную систему нет подробной информации в широком доступе, но по описанию функциональности, которое приводят разработчики в [5], можно сделать вывод, что выделенные подходы интеграции СЗИ с ALD также будут применимы к новой версии ALD Pro.

Программное обеспечение, реализующее функционал единого пространства пользователей (ЕПП), является уязвимым [6, 7] по отношению к внешним угрозам, поскольку механизмы реализации базируются на публичном протоколе и сам сервис является общедоступным, в том числе для злоумышленников. По этой причине целесообразна реализация механизма повышения защищенности сервиса ЕПП в части И/А.

Прежде чем приступить к рассмотрению определенных подходов интеграции СЗИ и ALD, про-

Лобач Андрей Олегович, студент.
E-mail: andrey.lobach@mail.ru

Статья поступила в редакцию 3 августа 2021 г.

ведем краткий обзор службы каталогов ALD и представим общую схему И/А СЗИ линейки Аккорд.

Служба каталогов ALD

Комплекс программ ALD предназначен для организации ЕПП для автоматизированных систем, работающих под управлением ОС Astra Linux.

ALD использует протокол прикладного уровня LDAP (Lightweight Directory Access Protocol), сетевой протокол аутентификации Kerberos 5, сетевую файловую систему CIFS (Common Internet File System) и решает следующие задачи [8]:

- централизованное хранение и управление учетными записями пользователей и групп;
- сквозную аутентификацию пользователей в домене с использованием протокола Kerberos 5;
- функционирование глобального хранилища домашних директорий, доступных по Samba/CIFS;
- автоматическую настройку всех необходимых файлов конфигурации UNIX, LDAP, Kerberos;
- поддержку соответствия БД LDAP и Kerberos;
- создание резервных копий БД LDAP и Kerberos с возможностью восстановления;
- интеграцию в домен входящих в дистрибутив ОС Astra Linux СУБД, серверов электронной почты, веб-серверов, серверов печати и т. п.

Обобщенная схема И/А в СЗИ

Для формирования возможных подходов механизма интеграции СЗИ в ALD необходимо выделить общую схему И/А в СЗИ.

Исходя из анализа механизмов конкретных видов реализации И/А можно выделить следующие этапы [2], [9, 10]:

1) ввод данных АИП (аутентифицирующая информация пользователя) и учетной информации пользователя;
2) передача в обработку;
3) преобразование данных. Получение данных для сравнения с эталоном (идентификаторы, хэши паролей);
4) получение эталонов из базы;
5) хранение эталонов;
6) сравнение с эталоном плюс дополнительные проверки;
7) принятие решения об успешности И/А;
8) хранение прав пользователя;
9) получение прав пользователя;
10) принятие решения о доступе и правах;
11) предоставление доступа.

При этом регистрация нового пользователя в СЗИ осуществляется следующим образом:

- администратор присваивает пользователю уникальное имя в системе;
- происходит настройка параметров учетной записи пользователя:
  - персональный идентификатор;
  - пароль;
  - данные аутентификации.

Дополнительно можно выполнить настройку следующих параметров [8, с. 17]:

- параметры пароля;
- атрибуты доступа;
- результаты И/А.

Предлагаемые подходы по интеграции СЗИ с ALD

С учетом обобщенной схемы И/А СЗИ и функционала ALD выделим следующие подходы.

Использование ALD как инструмента идентификации/аутентификации. Идея использования службы каталогов как способа аутентификации возникла из анализа источника [11]. В [11] в качестве службы каталогов выступает AD. Поскольку в основе AD и ALD лежат реализации протокола LDAP, выбор данного подхода применительно к ALD представляется перспективным.

При использовании данного подхода необходимо дублировать хранилище пользователей в СЗИ и ALD, поскольку при прохождении И/А ALD необходимо подтверждать введенный пароль пользователя, т. е. данные о пользователях обязательно должны сохраняться и в ALD. Соответственно этапы 2—7 (непосредственно аутентификация) обобщенной схемы И/А в СЗИ дублируются в ALD. Авторизация пользователя происходит исключительно на стороне СЗИ (этапы 8—11).

Регистрация нового пользователя происходит и в СЗИ, и в ALD. При этом в ALD сохраняется только та информация, которая требуется для аутентификации (идентификаторы, хэши паролей).

Реализация предполагает создание информационной системы, которая позволит осуществлять ведение информации о пользователях в СЗИ и проведение И/А на стороне ALD, одновременно с этим при регистрации новых пользователей в ALD позволит обновлять матрицу доступа в СЗИ.

Предлагаемый алгоритм работы информационной системы следующий:

- получаем идентификатор пользователя;
- посредством Kerberos подтверждаем существование такого пользователя в ALD;

- если пользователь зарегистрирован в ALD, СЗИ запрашивает пароль, в противном случае выдается сообщение об ошибке и процесс аутентификации прерывается;
- введенный пароль используется для аутентификации пользователя посредством СЗИ.

Недостатком данного подхода является необходимость обеспечения синхронизации данных пользователей между базами данных СЗИ и ALD, а также дублирование хранилища пользователей, что может отрицательно повлиять на уровень защищенности всей системы.

Кроме того, происходит некоторое снижение быстродействия из-за необходимости взаимодействия распределенных систем, а также возникает задача администрирования/поддержки работы инфраструктуры (на узлах должна быть обеспечена установка единого времени) [12].

Хранение базы данных СЗИ в облаке, т. е. полное перенесение данных в ALD. Возможность работы с атрибутами пользователя ALD подтверждается наличием доступных библиотек для доступа к публичным интерфейсам OpenLDAP в составе ALD [13]. Появляется возможность хранения вне контура СЗИ данных пользователя, которые необходимы для выполнения процедуры И/А.

При таком подходе данные пользователя хранятся в ALD. При предъявлении пользователем идентификатора СЗИ обращается к ALD. В случае введения существующего идентификатора ALD передает в СЗИ данные о пользователе (например, хэш-пароль) для последующей аутентификации. Если пользователь вводит верный пароль, аутентификация считается пройденной.

При использовании данного подхода СЗИ делегирует ALD этапы 4, 5 обобщенной схемы И/А СЗИ (хранение и получение эталонов), а также этапы 8, 9 (хранение и получение прав пользователей).

Соответственно регистрация нового пользователя осуществляется в СЗИ, но при этом результаты регистрации сохраняются в ALD.

Реализация предполагает создание информационной системы, которая позволит хранить и получать данные о пользователях из ALD и при этом выполнять операции И/А на стороне СЗИ.

Предлагаемый алгоритм работы системы следующий:

- получение идентификатора пользователя;
- выполнение запроса в базу данных ALD в целях получения атрибутов пользователя, необходимых для проведения процедуры аутентификации (например, хэш-пароля);
- в случае, если данный пользователь обнаружен в базе данных ALD, проведение аутентификации пользователя посредством СЗИ;
- если введенный пароль совпал, процесс аутентификации успешно завершается.

В данном подходе все данные хранятся в ALD, соответственно, увеличивается вероятность их компрометации.

При этом не задействуются механизмы И/А ALD, поэтому данный подход является менее защищенным, чем альтернативные.

Данные о пользователях остаются локальными и синхронизируются с данными в ALD. В соответствии с аргументами, описанными ранее, наличие публичных интерфейсов OpenLDAP [13] позволяет осуществлять синхронизацию данных пользователей в ALD и СЗИ.

Актуальные данные пользователя хранятся в ALD. Периодически эти данные копируют в локальное хранилище СЗИ. При предъявлении пользователем идентификатора СЗИ обращается к локальной базе. В случае, если в локальной базе данные не обнаружены, выполняется запрос в ALD для их обновления по конкретному идентификатору. Если требуемый идентификатор пользователя существует, СЗИ выполняет запрос пароля. После этого происходит аутентификация пользователя по данным из хранилища.

Таким образом, в данном подходе в ALD дублируются 4-й и 5-й этапы обобщенной схемы И/А СЗИ (хранение и получение эталонов), а также 8-й и 9-й этапы (хранение и получение прав пользователей).

Регистрация нового пользователя осуществляется на стороне СЗИ, после чего результат регистрации сохраняется в ALD. При входе этого пользователя локальная база СЗИ будет обновлена путем обмена данными с ALD.

Для реализации указанного подхода необходимо создание системы, которая выполняет периодическую или по событию (в случае ошибок, связанных с данными из локальной базы) синхронизацию данных по пользователям из ALD в локальную базу.

Предлагаемый алгоритм работы системы следующий:

- получение идентификатора пользователя;
- выполнение запроса в локальную базу данных СЗИ для осуществления идентификации;
- в случае, если в локальной базе идентификатор пользователя не обнаружен, выполнение запроса в базу данных ALD. При этом в локальную базу данных СЗИ происходит копирование актуальной информации по пользователю;

- в случае успеха (идентификатор существует) осуществляется запрос пароля пользователя и начинается выполнение процедуры аутентификации;
- в случае ошибки аутентификации снова происходят обращение к базе данных ALD и обновление информации в локальной базе по конкретному пользователю для обработки случаев, когда пароль пользователя был изменен в ALD, но синхронизация с локальным хранилищем еще не выполнена;
- если введенный пароль совпал, процесс аутентификации успешно завершается.

При данном подходе синхронизация осуществляется за счет периодического опроса данных пользователей в ALD, и в случае, если интервал опроса недостаточно короткий, синхронность данных в СЗИ и ALD может быть нарушена.

Показательным примером такого нарушения является то, что реализация допускает возможность успешной аутентификации пользователя, который был удален в ALD.

Данный подход является лучшим с точки зрения быстродействия, но более сложным в реализации, чем альтернативные варианты.

Заключение

Каждый из приведенных подходов имеет свои преимущества и недостатки. При этом можно выделить ряд угроз, касающихся всех походов: угрозы, связанные с доверием к маршруту и каналу СЗИ—ALD, а также угрозы, связанные с корректной работой управления атрибутами безопасности (идентификаторы, группы, роли и т. д.) [11]. Также можно выделить общую проблему, которая заключается в том, что все эталоны хранятся в ALD, что является уязвимым местом приведенных подходов. Однако для первого подхода эта уязвимость наименее критична, поскольку атрибуты доступа хранятся только в СЗИ.

Первый подход, использующий возможности ALD для И/А, является самым защищенным, но неэффективным с точки зрения быстродействия, поскольку все обращения приводят к запросам в ALD.

Второй подход является также относительно медленным по тем же причинам, что и в первом случае. При этом он недостаточно защищен по сравнению с первым подходом.

Третий подход — самый быстродействующий по сравнению с альтернативными подходами, поскольку в нём минимизированы обращения к внешнему сервису (ALD) в процессе аутентификации. Однако данный подход допускает возможность ложной аутентификации.

По указанным причинам для реализации стоит выбирать между первым и третьим подходами в зависимости от того, что находится в приоритете: повышенная защищенность системы или ее быстродействие.

Литература

1. *Сухов Р., Исаев Е., Мальцева С.* Доклад "Экосистемы в информационных технологиях". — М., 2017. — 12 с.
2. *Щеглов А., Щеглов К.* Идентификация и аутентификация. Так ли все просто? [Электронный ресурс]. URL: https://ecm-journal.ru/post/Identifikacija-i-autentifikacija-Tak-li-vse-prosto.aspx (дата обращения: 22.05.2021).
3. *Богаченко Н. Ф.* Анализ проблем управления разграничением доступа в крупномасштабных информационных системах // Математические структуры и моделирование. 2018. № 2(46). С. 135—152.
4. Единая система идентификации и аутентификации в инфраструктуре электронного правительства РФ (ЕСИА) // Zdrav. Expert. 2020 [Электронный ресурс]. URL: https://zdrav.expert/index.php/Статья:Единая_система_идентификации_и_аутентификации_в_инфраструктуре_электронного_правительства_РФ_(ЕСИА) (дата обращения: 26.07.2021).
5. Презентация ALD Pro. [Электронный ресурс]. URL: https://astralinux.ru/information/materials/prezentacziya-ald-pro-resheniya-dlya-avtomatizaczii-czentralizovannogo-upravleniya.pdf (дата обращения: 26.07.2021).
6. *Ализар А.* Обход аутентификации в pam_ldap. 11 марта 2006 [Электронный ресурс]. URL: https://xakep.ru/2006/11/03/34885/ (дата обращения: 29.05.2021).
7. *Ализар А.* Обход ограничений безопасности в OpenLDAP. 9 июня 2006 г. [Электронный ресурс]. URL: https://xakep.ru/2006/09/06/33701/ (дата обращения: 29.05.2021).
8. Справочный центр Astra Linux [Электронный ресурс]. URL: https://wiki.astralinux.ru/display/doc/Astra+Linux+Directory (дата обращения: 29.05.2021).
9. ПАК СЗИ от НСД для ПЭВМ (РС) "Аккорд-АМДЗ". Руководство администратора. М.: ОКБ САПР, 2019. — 121 с. [Электронный ресурс]. URL: https://www.okbsapr.ru/upload/iblock/f86/f86fb0fdbaa07b51afa3cafc2c96eeda.pdf
10. ПАК СЗИ от НСД "Аккорд-Win64" (версия 5.0). Руководство администратора. М.: ОКБ САПР. — 101 с. [Электронный ресурс]. URL: https://www.okbsapr.ru/upload/iblock/e86/e86f0a022bb079b46f4e3a10375054d8.pdf
11. *Похачевский Д. А.* О некоторых угрозах СДЗ, использующих ACTIVE DIRECTORY для решения задач аутентификации и авторизации: мат. XXIV Научно-практ. конф. "Комплексная защита информации" Витебск. 21—23 мая 2019 г.: УО ВГТУ. — Витебск, 2019. С. 376—380.
12. *Шнайер Б.* Глава 3. Основные протоколы. Протокол Kerberos // Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си = Applied Cryptography. Protocols, Algorithms and Source Code in C. — М.: Триумф, 2002. С. 81.
13. *Yves Legrandgerard* libldap Documentation. Release 0.1. 2017 г. [Электронный ресурс]. URL: https://readthedocs.org/projects/libldap/downloads/pdf/stable/ (дата обращения: 29.05.2021).

Integration of Information Security System with the Astra Linux Directory service: problems and approaches

A. O. Lobach
Moscow Institute of Physics and Technology (National Research University), Dolgoprudny, Moscow region, Russia

In this article, a generalized scheme of identification/authentication (hereinafter referred to as I/A) of the Information Security System (ISS) is formulated. The Astra Linux Directory (ALD) is reviewed. Based on this, approaches to solving the problem of integration the ISS and ALD are proposed and considered. In each of the approaches, the stages I/A of ISS that pass to the ALD side during their integration are highlighted. General algorithms for the implementation of these approaches are formulated. The main problems and threats of the selected approaches are also identified.

Keywords: information security system, Astra Linux Directory, authentication, identification, threats.

Bibliography — 13 references. *Received August 3, 2021*